

Narrow-Bicliques: Cryptanalysis of Full IDEA

Dmitry Khovratovich, Microsoft Research
Gaetan Leurent, University of Luxembourg
Christian Rechberger, DTU MAT

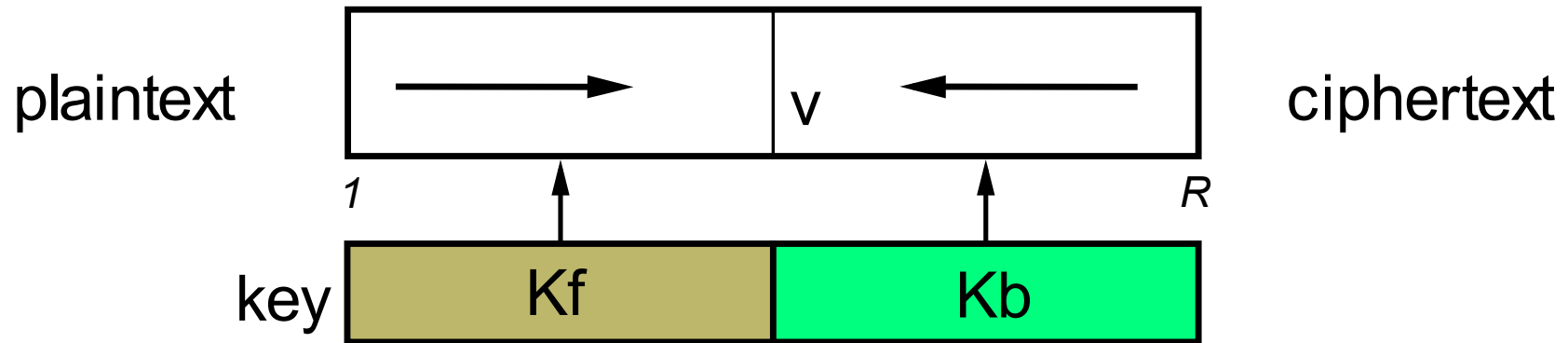
Cryptanalysis 101

- Differential attacks
- Linear attacks

Cryptanalysis 101

- Differential attacks
- Linear attacks
- Why? Powerful, versatile, found many applications since early 90s
- Many variants
- Impact on cipher design: proofs against classes of those attacks are state-of-the-art

Meet-in-the-middle attacks



- Overshadowed by differential and linear attacks in recent 20+ years
- Changing since attack on lightweight cipher KTANTAN (SAC 2010 and later)

Outline

- Setting
- Review of meet-in-the-middle attacks
- Description of IDEA
- Attacks on
 - 6 rounds (shortcut)
 - 7.5 rounds (shortcut)
 - Full 8.5 rounds (bruteforce-like)
- Conclusion and future work

The setting

- Given: A block cipher
- Goal: find the single unknown key
- Cryptanalyst is allowed to choose plaintexts and ask for their ciphertexts (CPA)

Brute-force:

guess all 2^k keys for success probability 1

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

MITM on 2-key 2-DES

Merkle-Hellman 81

MITM on 2-key 3-DES

Chaum-Evertse 85

6-7 rounds of DES

Hash functions

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Hash functions

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Hash functions

Lai-Massey 92

2nd-preimage on iterated constructions

Aoki-Sasaki et al. 08-10

Preimage for MD5, ...

Guo-R. et al. 10

Preimages for Tiger, ...

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

?



MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

KTANTAN Key-recovery

Wei-R. et al. 11

Improved KTANTAN

Key-recovery

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10



MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

*Improvements with „Biclique“
view: SHA-2, Skein*

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

?



*Improvements with „Biclique“
view: SHA-2, Skein*

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Bogdanov-Khovratovich-R.

New AES Results

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

*Improvements with „Biclique“
view: SHA-2, Skein*

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Bogdanov-Khovratovich-R.

Khovratovich-Leurent-R.

New IDEA Results

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

*Improvements with „Biclique“
view: SHA-2, Skein*

MITM attacks on Symmetric Primitives

Block ciphers

Diffie-Hellman 77

Merkle-Hellman 81

Chaum-Evertse 85

Bogdanov-R. 10

Wei-R. et al. 11

Bogdanov-Khovratovich-R.

Khovratovich-Leurent-R.

New IDEA Results

Hash functions

Lai-Massey 92

Aoki-Sasaki et al. 08-10

Guo-R. et al. 10

Khovratovich-R.-Savelieva 12

*Improvements with „Biclique“
view: SHA-2, Skein*

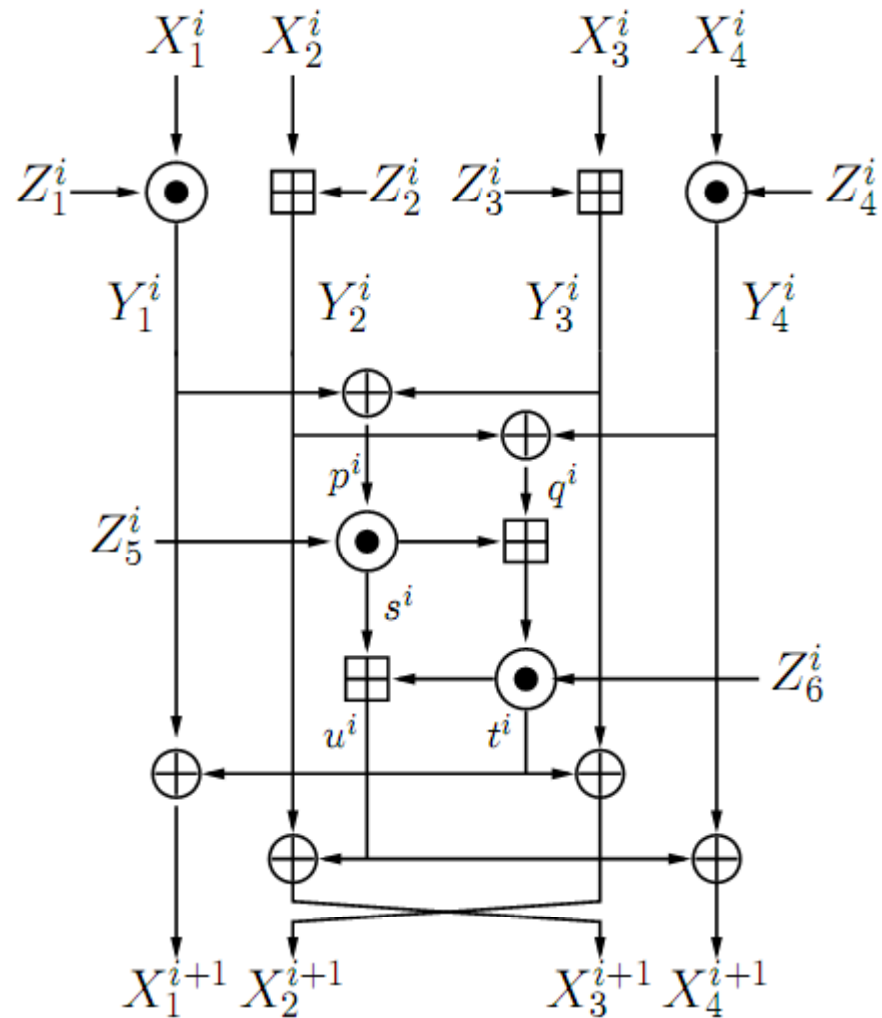
The Biclique approach

- Formalization of „Initial structure“ concept due to Aoki-Sasaki 09
- Mapping to differential framework possible and intuitive
 - Differential characteristics/trails
 - Neutral bits
 - Rebound techniques
- Analyzing more rounds possible

IDEA

- Designed by Lai and Massey, 91
- 64-bit blocks, 128-bit key
- Widely implemented
- 20+ research papers
- So far: best published result on 5/6 out of 8.5 rounds by Sun-Lai 09:
 - first 5-round: 2^{17} data and $2^{125.5}$ time or 2^{64} data and 2^{115} time
 - middle 6-round: better results

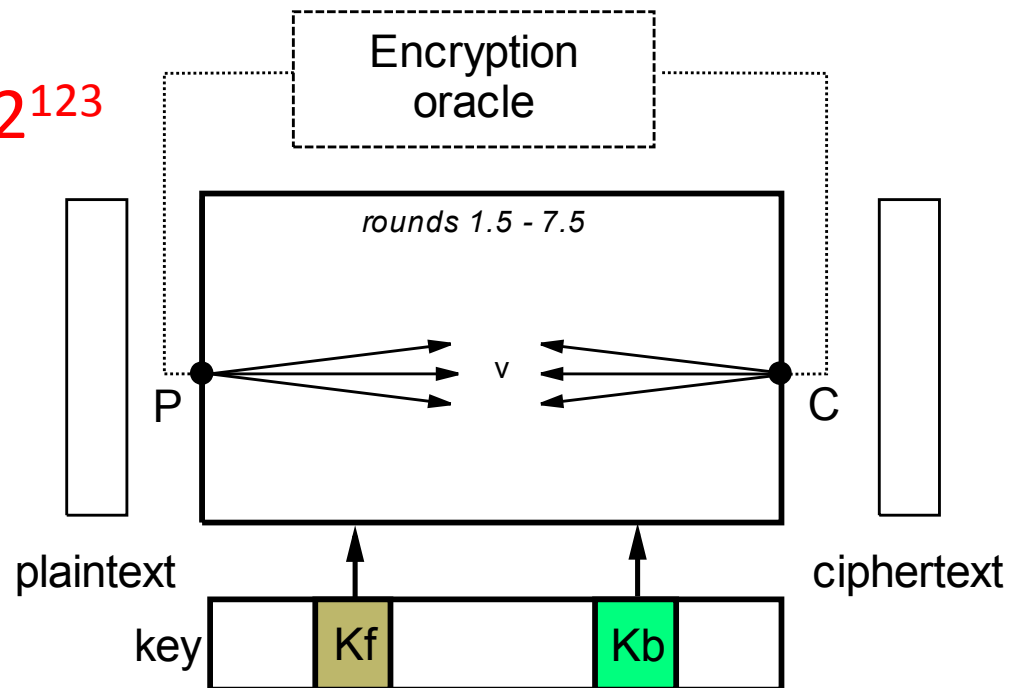
IDEA Round



MITM on IDEA

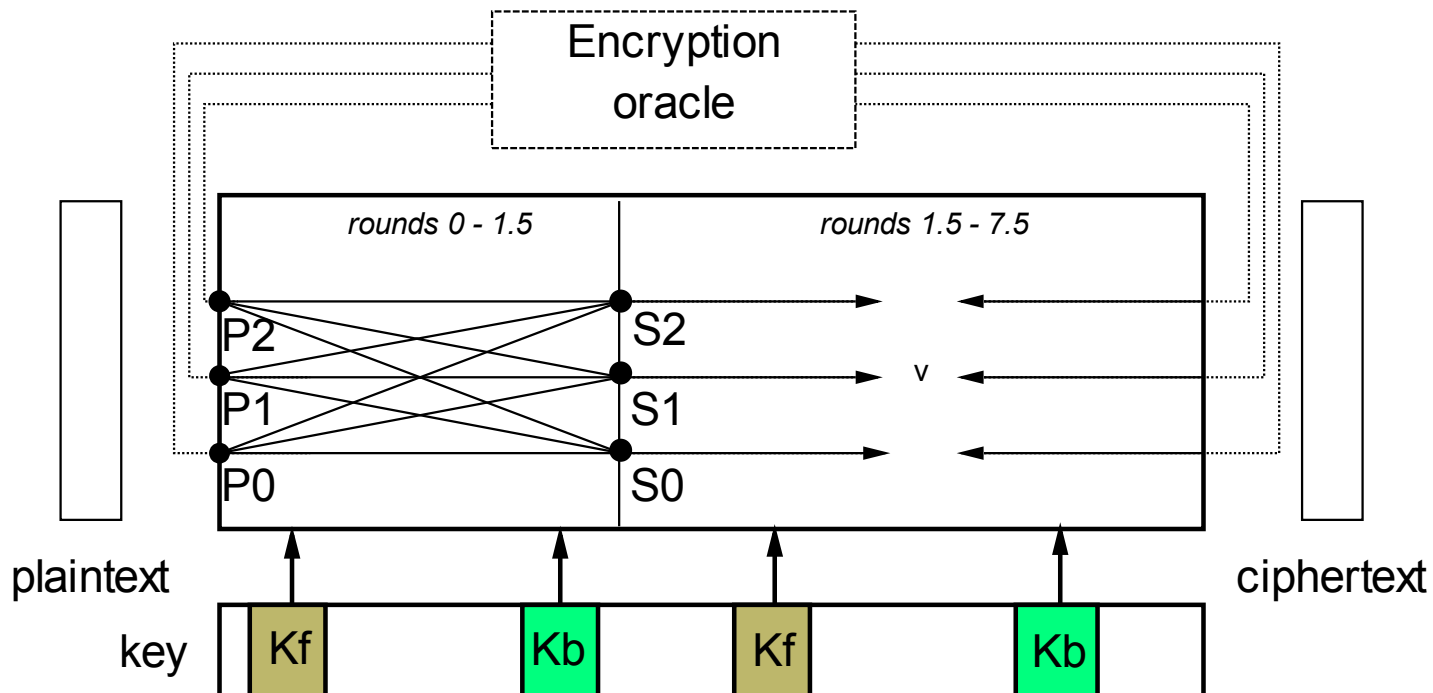
- Crypto 2011 Rump Session, Biham et al.: MITM attacks on up to 6 (middle) rounds
- Example: variant with 2 plaintext/ciphertext pairs

– Time: about 2^{123}



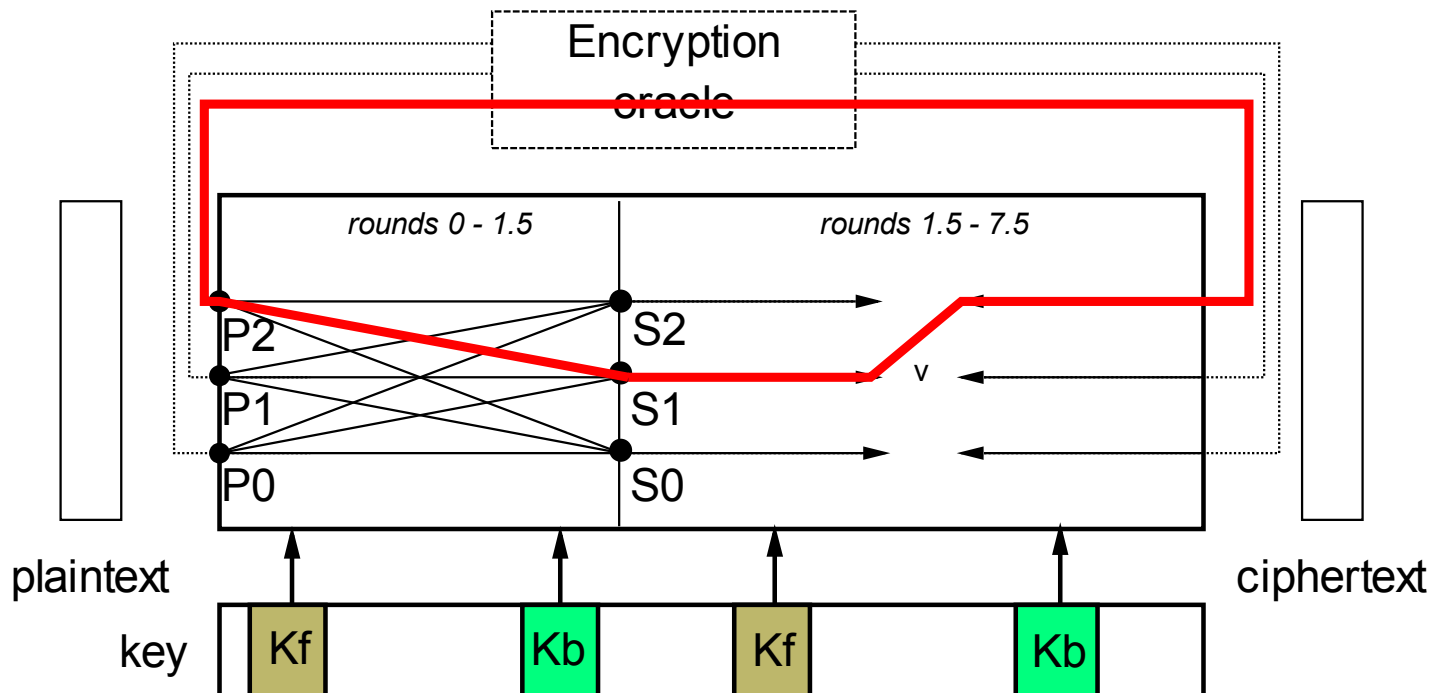
Bicliques and IDEA

- Initial biclique result: attack on 7.5 rounds
- Problem: Half of codebook needed
- Time: **again** about 2^{123}



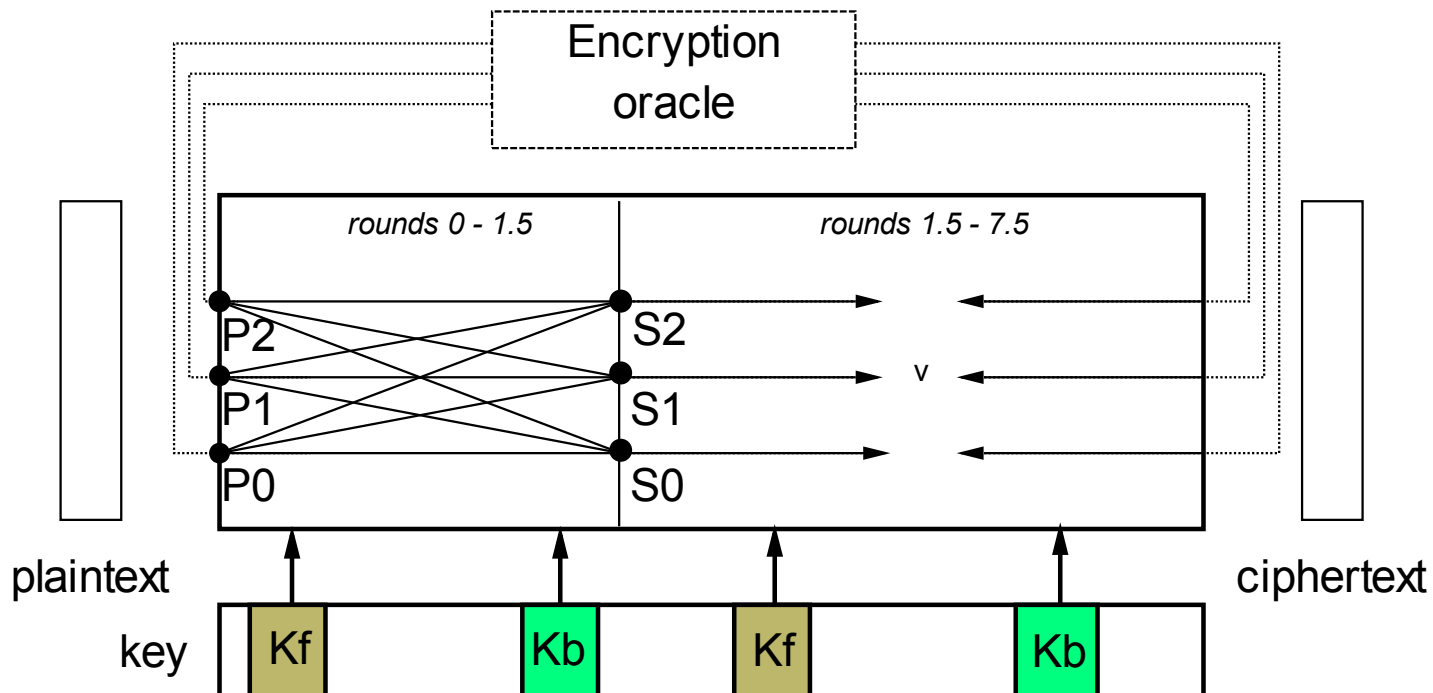
Bicliques and IDEA

- Initial biclique result: attack on 7.5 rounds
- Problem: Half of codebook needed
- Time: **again** about 2^{123}



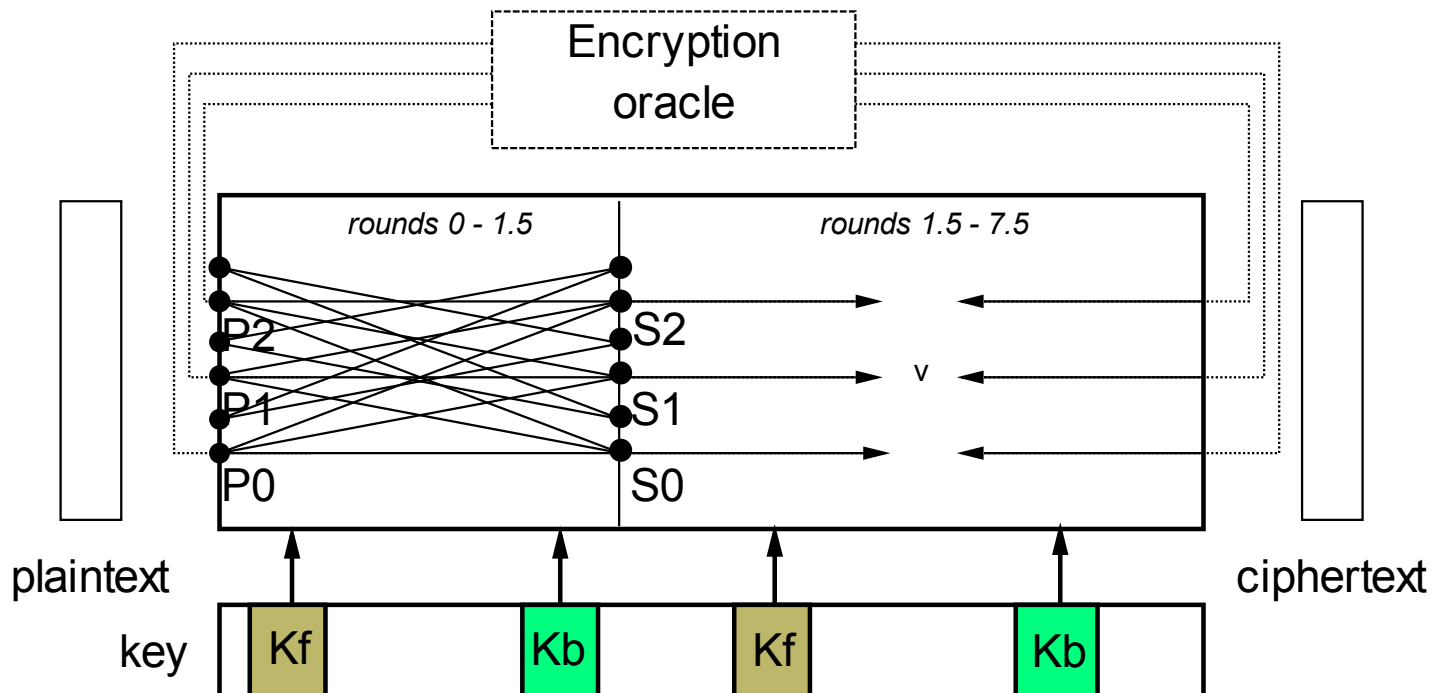
Bicliques and IDEA

- Initial biclique result: attack on 7.5 rounds
- Problem: Half of codebook needed
- Time: **again** about 2^{123}



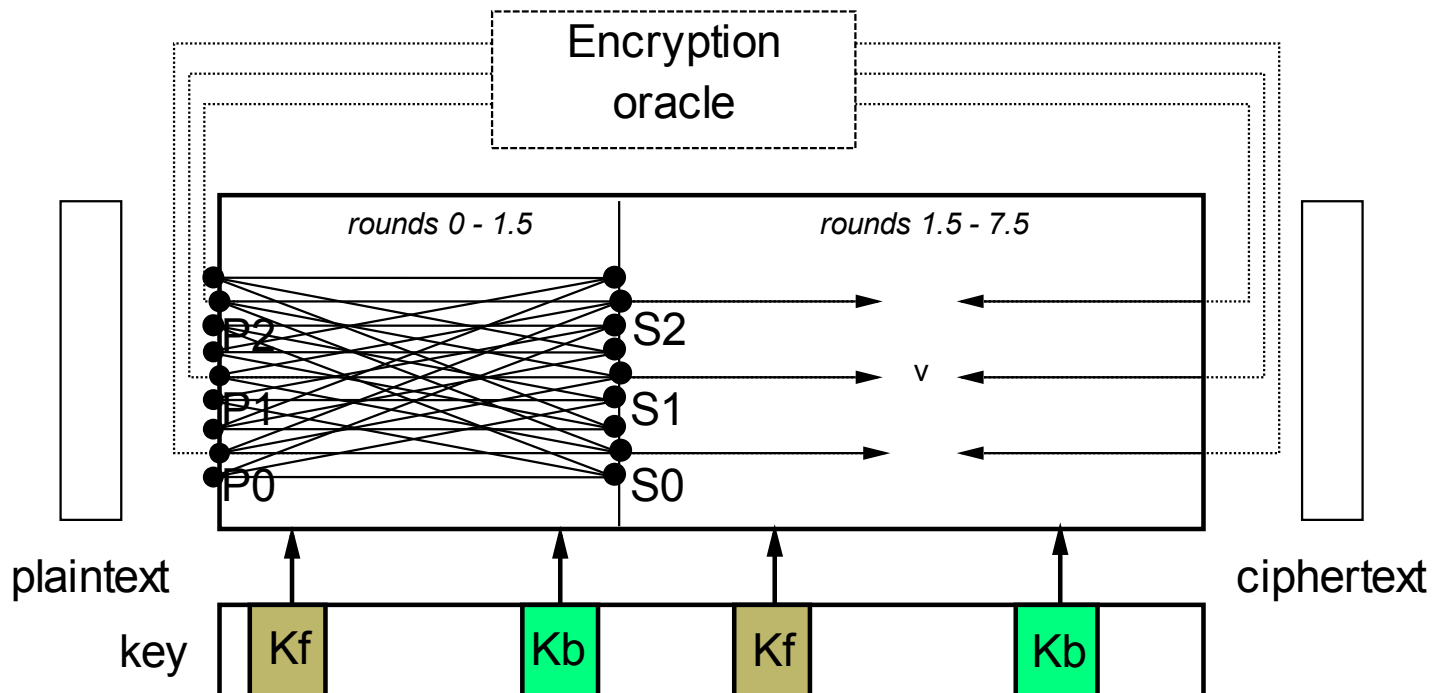
Bicliques and IDEA

- Initial biclique result: attack on 7.5 rounds
- Problem: Half of codebook needed
- Time: **again** about 2^{123}



Bicliques and IDEA

- Initial biclique result: attack on 7.5 rounds
- Problem: Half of codebook needed
- Time: **again** about 2^{123}



Narrow Bicliques and IDEA

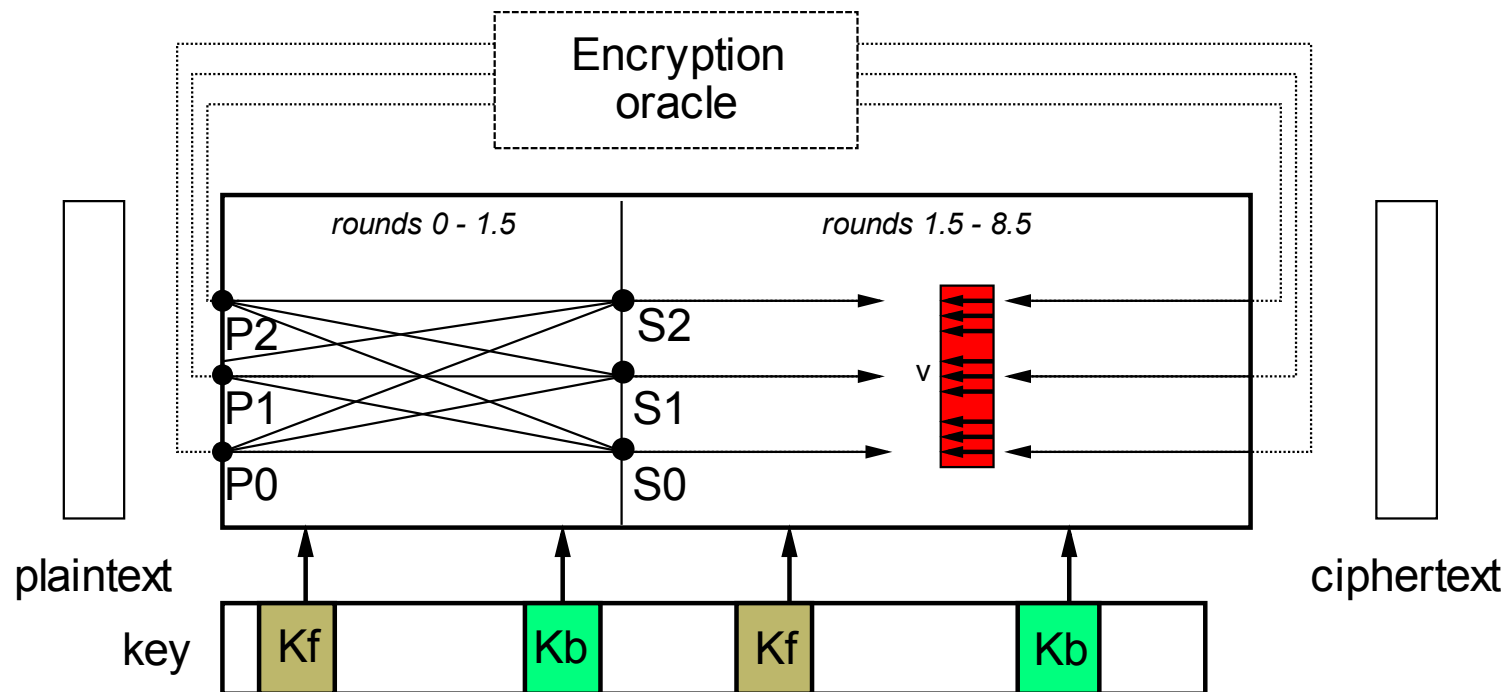
- Address the problem of exploding data requirements
- **New tricks:**
 - Efficiently, for every key group, find internal state variables such that resulting plaintexts collide in as many bits as possible
 - Multiple bicliques per key group
- Can be complicated: **practically verified**

Examples of results (those minimizing time complexity)

Rounds	Data complexity Biclique	Data complexity Narrow Biclique	time
first 5	63	25	101,5
first 6	63	41	118,9
first 7.5	63	52	123,9

Narrow Bicliques and full IDEA

- Next biclique application: attack on full 8.5 rounds. **1-round brute-force in matching part.**
- Time: about 2^{126}



More examples of results

Rounds	Data complexity Biclique	Data complexity Narrow Biclique	time
first 5	63	25	101,5
first 6	63	41	118,9
first 7.5	63	52	123,9
full (8.5)	63	59	125,97
full (8.5)	63	52	126,06

Conclusions

- Two main contributions:
 - Much improved cryptanalysis (reduced) IDEA
 - See also recent update of Biham et al. eprint 2011/417
 - New tool for the biclique framework
- Biclique attacks **million times faster than brute-force** for reduced-round variants
- Broken? If AES is „broken“, then so is IDEA (also about **126 bit security**)

Open Problems

- More ideas from hash cryptanalysis applicable to cipher cryptanalysis?
- New variants of and targets for biclique cryptanalysis
- Explore new sub-discipline:

bruteforce-like cryptanalysis

Interesting case: Improve optimized brute-force attacks on ciphers with **80-bit keys (or less)**

Narrow-Bicliques: Cryptanalysis of Full IDEA

Q&A

Dmitry Khovratovich, Microsoft Research

Gaetan Leurent, University of Luxembourg

Christian Rechberger, DTU MAT